20-MJ-6781-MPK
20-MJ-6782-MPK
20-MJ-6783-MPK
20-MJ-6784-MPK

AFFIDAVIT OF SPECIAL AGENT JACQLEEN CUNNINGHAM IN SUPPORT OF APPLICATIONS FOR TWO CRIMINAL COMPLAINTS AND TWO SEARCH WARRANTS

I, Jacqleen Cunningham, being duly sworn, hereby depose and state as follows:

Agent Background

1. I am a Special Agent with Homeland Security Investigations ("HSI") and have been so employed since June 2010. I have successfully completed a training program in conducting criminal investigations at the Federal Law Enforcement Training Center in Brunswick, Georgia. In 2007, I graduated from Sacred Heart University with a Bachelor of Science Degree in Criminal Justice. My current assignment as an HSI Special Agent includes conducting and participating in investigations involving the fraudulent acquisition, production, and misuse of United States immigration documents, United States passports, and various identity documents. Due to my training and experience, as well as conversations with other law enforcement officers, I am familiar with the methods, routines, and practices of document counterfeiters, vendors, and persons who fraudulently obtain or assume false identities.

2. I am also a member of HSI's Document and Benefit Fraud Task Force ("DBFTF"), a specialized field investigative group comprised of personnel from various local, state, and federal agencies with expertise in detecting, deterring, and disrupting organizations and individuals involved in various types of document, identity, and benefit fraud schemes. The DBFTF is currently investigating a group of suspects who are believed to have obtained stolen identities of other United States citizens from Puerto Rico and elsewhere. Many of these

individuals used the stolen identities to open bank accounts and/or credit cards to fraudulently purchase, register, and/or export vehicles as part of a multi-state scheme involving financial fraud, auto theft, and the exportation of stolen goods.

3. I am submitting this affidavit in support criminal complaints charging Darwyn JOSEPH ("JOSEPH"), date of birth xx-xx-1996, and Ramon Joseph CRUZ ("CRUZ"), date of birth xx-xx-1996, with conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349, and aggravated identity theft, in violation of 18 U.S.C. § 1028A (the "Target Offenses").

4. I also submit this affidavit in support of an application for search warrants for the following properties: 445 S Broadway, Lawrence, Massachusetts ("Target Location 1"), as described more fully in Attachment A-1 and 66 Pleasant Street 2, Methuen, Massachusetts ("Target Location 2"), as described more fully in Attachment A-2. I have probable cause to believe that these properties contain evidence, fruits, and instrumentalities of the Target Offenses, as described in Attachments B-1 and B-2.

5. The facts in this affidavit come from my personal involvement in this investigation, including interviews of witnesses, and my review of documents and bank records, as well as my conversations with other members of law enforcement. In submitting this affidavit, I have not included every fact known to me about this investigation. Instead, I have only included facts that I believe are sufficient to establish probable cause.

Background of Investigation

6. Since approximately January 2019, HSI special agents have been investigating a scheme involving the use of stolen identities to fraudulently open bank accounts, obtain credit cards, and purchase vehicles, many of which are then exported out of the United States. More specifically, the investigation has revealed a number of individuals using the stolen identities of

United States citizens from Puerto Rico to fraudulently finance late-model vehicles from dealerships in Massachusetts, paying zero dollars down. At the dealerships, the individuals provide a variety of fraudulent identification and credit-related documents, including fraudulent Puerto Rico driver's licenses and social security cards as proof of identification. The perpetrators of this fraudulent scheme typically do not make payments on the vehicles, resulting in the dealership or relevant lending financial institution taking a total loss for the vehicles. The individuals have also been successful in opening bank accounts in the same stolen identities prior to fraudulently purchasing the vehicles. Individuals perpetrating the scheme max out associated credit cards within days or weeks and rarely make any payments on the accounts. Recent investigation has also revealed that some of these same individuals – along with JOSEPH and CRUZ – were also involved in a scheme to use stolen identities to open bank accounts, to apply for Economic Injury Disaster Loans ("EIDLs") from the United States Small Business Administration ("SBA") and elsewhere, to accept funds from those loans through transfers into the fraudulent bank accounts, and to launder the funds.

Probable Cause

Background of Investigation; Identification of JOSEPH and CRUZ as Co-Conspirators with Rivera and Others

7. On or about September 9, 2020, HSI Special Agent Timothy Taber, with whom I am working on this investigation, submitted to this court an affidavit in support of a criminal complaint charging Alvin RIVERA ("RIVERA"), with false representation of a social security number, in violation of 42 U.S.C. § 408(a)(7)(B), and aiding and abetting the same, in violation of 18 U.S.C. § 2; aggravated identity theft, in violation of 18 U.S.C. § 1028A, and aiding and abetting the same, in violation of 18 U.S.C. § 2; and wire fraud, in violation of 18 U.S.C. § 1343. In addition, the affidavit supported an application for a search warrant for 15 Brockton

Avenue, Haverhill, Massachusetts. *See* 20-MJ-6557-MPK and 20-MJ-6560-MPK. A copy of Special Agent Taber's affidavit is attached to this affidavit as Exhibit 1 and incorporated by reference as though fully set forth herein. On September 9, 2020, this Court found probable cause and granted the applications for arrest and search warrants.

8. On September 10, 2020, DBFTF agents and officers executed federal arrest and search warrants at 15 Brockton Ave in Haverhill, MA. Based on the investigation to date, and the nature of the ongoing offenses, agents expected to uncover numerous fraudulent documents, stolen profiles, personal identifying information ("PII") and financial information related to stolen identities at RIVERA's residence.

9. As a result of the search, agents did discover these types of documents and information, including approximately twenty-nine fraudulent driver's licenses, and many of their accompanying social security cards and debit/credit cards. The majority of the driver's licenses contained different identities, yet contained photographs of the same nine individuals, three of which depicted JOSEPH[1]. The licenses depicting JOSEPH were discovered in three places: (1) an Adidas bag in the kitchen (New Hampshire driver's license in the name of D.P.C.[2]), (2) hidden within a hairbrush in the bathroom (New Jersey driver's license in the name of G.F.O.[3]), and (3) hidden within a hairbrush in the Infiniti SUV in the driveway (New Jersey driver's license in the name of A.T.L.[4]). Also discovered hidden within a hairbrush in the

[1] After comparing these photographs to JOSEPH's photograph contained on file with the Massachusetts Registry of Motor Vehicles and his Passport photograph, agents confirmed that the photographs on the three fraudulent licenses depict JOSEPH.

[2] The identity of victim D.P.C. is known to the government. In order, these initials represent the victim's first name, middle name and last name. To protect the victim's privacy, only the initials "D.P.C." and D.C." are used in this affidavit to reflect the variations of the victim's full name that were used by JOSEPH.

[3] The identity of victim G.F.O. is known to the government. In order, these initials represent the victim's first name, paternal last name and maternal last name.

[4] The identity of victim A.T.L. or A.L. is known to the government. In order, these initials represent the victim's first name, paternal last name and maternal last name.

Infiniti SUV was a KeyBank credit/debit card in the name of R.T.L., which is an identity used by CRUZ and is more fully discussed throughout this affidavit.

10. During the search, agents and officers located a social security card with an issuance date of 06/12/2020 in the name of JOSEPH on the desk in a room labeled "restricted area." As described more fully below, DBFTF members also located several money service business receipts from targets of the investigation to individuals in the Dominican Republic within a red bag in the kitchen of RIVERA's residence.

a. Two receipts listed JOSEPH, of 445 S Broadway St. Lawrence, MA 01843 (Target Location 1), as the sender. One of the receipts indicated that on September 9, 2020 at approximately 5:34pm, JOSEPH transferred $970.00 to a female in the Dominican Republic ("Person One"). The second receipt in JOSEPH's name indicated that he transferred $970 to the Dominican Republic from Lawrence, MA on September 9, 2020 at approximately 5:45 pm (*i.e.*, about 12 minutes after the first transfer).

b. Other receipts seized during the warrant documented Person One received wire transfers from other targets of this investigation. On September 3, 2020, someone using the name I.H.C.[5] transferred $970.00 to Person One. During the search of RIVERA's residence, agents and officers located a Pennsylvania driver's license in the name of I.H.C. The license depicted Neida LOPEZ. LOPEZ was arrested, as part of this investigation, on September 10, 2020 and indicted on charges of conspiracy to commit

[5] The identity of victim I.H.C. is known to the government. In order, these initials represent the victim's first name, paternal last name and maternal last name.

wire fraud and aggravated identity theft on September 29, 2020, in *United States v. Neida Lopez,* 20-CR-40035.

c. Two receipts listed "Ramon Joseph Jr Cruz" as the sender to a recipient in the Dominican Republic; in both transactions, $970 was the amount transferred. One receipt was dated September 9, 2020 at 5:33 pm, and the other was dated September 9, 2020 at 5:36 pm. Both transfers were made from a store on the same street in Lawrence, MA as one of the JOSEPH transactions. Agents believe LOPEZ, using the I.H.C. identity, and JOSEPH and CRUZ using their true identities, made these wire transfers to the Dominican Republic under the direction of RIVERA, in furtherance of the conspiracy further described below.

11. Agents also seized seven Chime[6] Debit/Visa cards during the search of RIVERA's residence. The Chime Cards were discovered in two places: (1) a red Nike bag in the kitchen, and (2) on the kitchen table. In addition to the physical Chime cards, an iPhone cell phone belonging to RIVERA was seized and subsequently searched pursuant to the warrant. Within the phone, agents located the identifiers for approximately 27 additional Chime accounts to include one account in the D.P.C. identity that was used by JOSEPH. RIVERA's phone contained details of Chime accounts including, but not limited to the account holder's name, address, date of birth, social security number, account number, routing number, password and pin. The notes also listed which external bank accounts were linked to the Chime accounts, which is discussed further in paragraphs 37-42.

[6] According to its web site, Chime is a financial technology company. It connects users to bank services provided by The Bancorp Bank or Stride Bank, N.A.

JOSEPH's Acts in Furtherance of the Conspiracy and Scheme to Defraud

JOSEPH's Use of A.T.L. Identity Generally

12. On or about October 14, 2020, HSI Special Agents conducted a forensic analysis of RIVERA's iPhone that was seized on September 10, and discovered a June 19, 2020 WhatsApp message from RIVERA to a contact saved as "$ ANDERSON $," who used cell phone number (860) 313-8004.[7] The message contained the PII pertaining to the same A.T.L. identity on the New Jersey driver's license discussed in paragraph 9 that depicted a photograph of JOSEPH. The text of the message is as follows:

> A.T.L. 66 Linden St. Apt 2 Torrington, CT 06790-6719
> Been in residence 5Y 7M
> Monthly rent: $950
> DOB: xx/xx/1976 AGE: 43
> SSN: xxx-xx-1810
> Phone: 860-313-8004
> Email: TXXXXXtilingpros76@gmail.com
> Mailing Address: 167 Cherry St. Ste. 197, Milford, CT 06460
> Business Name: TXXXXX Tiling Pros
> Been in Business: 5Y 6M
> Annual Income: $214,000
> Monthly Income: $17,833

Based on my familiarity with this investigation, I know that RIVERA would commonly message "profiles" containing stolen identity information and additional made-up biographical details to co-conspirators so they could "study" the stolen identity prior to using it. I also know RIVERA would typically send the profile information to a "burner phone" used by the individual so that the individual could reference the information while inside a bank or store if they forgot any of the information. In this investigation, RIVERA and his associates likely provided JOSEPH with a burner phone using the phone number from the fraudulent A.T.L.

[7] The victim A.T.L.'s first name is Anderson. In this investigation, I have seen that RIVERA often saves in his phone the number of the "burner phone" associated with an identity theft victim's profile, and saves that contact under the identity theft victim's first name.

"profile" (860-313-8004) while JOSEPH was using the A.T.L. identity.

13. The above message from RIVERA to JOSEPH using the $ ANDERSON $ phone, also contained personal banking information in the A.T.L. identity regarding various bank accounts. Additionally, RIVERA saved specific details in his iPhone related to financial accounts in the A.T.L. identity, one of which is listed below.

> Chase Bank Personal Checking Account:
> Date Opened: July 27, 2020
> Opening Deposit: $25
> Online Banking Username: xxxxxxtilingpros76
> Password: xxxxxxxxxx
> Account#: xxxxxx360
>
> Blaky 818[8]

As described below, I believe that JOSEPH used the A.T.L. identity to, among other things, open bank accounts and receive funds obtained through a conspiracy with RIVERA.

JOSEPH's Use of A.T.L. Identity to Open a Fraudulent Bank Account

14. On or about July 27, 2020 – about one month after RIVERA sent JOSEPH the A.T.L. profile above on the $ ANDERSON $ burner phone – at approximately 2:00 p.m., a man appeared in person at a Chase bank branch in Avon, Connecticut and provided personal identifying information on a bank application in order to open a Chase total checking account. On the application, the applicant represented himself as A.T.L. with a date of birth of xx-xx-1976 and social security number xxx-xx-1810. The applicant provided an address of 66 Linden St., Apt 2 Torrington, CT, and phone number 860-313-8004 (the A.T.L. burner phone number). During the account opening process, the applicant presented a New Jersey driver's license with

[8] After reviewing the contents of RIVERA's phones, I have learned he commonly notates a version of an individual's true name/nickname below a fraudulent identity followed by a number. It is believed RIVERA did this to keep track of which criminal associate was utilizing a particular profile. In this case, RIVERA's notes indicated "BLAKY" – which I have learned in my investigation is a nickname or alias for JOSEPH – was using the A.T.L. identity, which was associated with an 818 credit score.

license number ending in -8762, date of birth of xx-xx-1976, issuance date of 08/07/2019, and expiration date of 08/31/2023. The applicant also provided a social security card bearing social security number xxx-xx-1810. After seizing the New Jersey driver's license in the A.T.L. identity but depicting JOSEPH's face, and the social security card in A.T.L.'s identity, from RIVERA's residence, and comparing them to the documentation provided by the applicant at Chase Bank, agents determined the license number, issue date, expiration date and social security number are the same. The applicant successfully opened checking account number xxxxxx360 with Chase Bank.

15. RIVERA's cell phone also contained detailed notes on a Bank of America account opened in the A.T.L. identity as follows:

> Bank of America Personal Account:
> Date Opened: July 23, 2020
> Opening Deposit: $25
> Online Banking Username: xxxxxxtilingpros76
> Password: xxxxxxxxxx
> Account#: xxxx-xxxx-1335
> Debit Card #: xxxx xxxx xxxx 4742
> Got Approved for $8,000 CC

16. On August 21, 2020 at approximately 3:31 p.m., RIVERA messaged the contact he had saved on his phone/in his WhatsApp account as "$ BLAKY $," at phone number 978-416-1355,[9] a photograph of a Bank of America letter addressed to A.T.L. of 167 Cherry St. Ste. 197, Milford, CT 06460. Along with the photograph RIVERA said, "Yo blacky that letter is from BOFA from an application for a BANK OF AMERICA TRAVEL REWARDS CC I put in through the online banking on Anderson's phone when I had it. I basically put all the info on the profile so alls the same if they ask questions. When u get a chance call the phone number on that

[9] From the context, I believe this phone number to be JOSEPH's personal phone number as opposed to the A.T.L. burner phone number saved as $ ANDERSON $. Additionally, a photograph of JOSEPH is associated to the WhatsApp profile of (978) 416-1355.

paper their giving us n let them know u receive a letter from them with a reference number: 4110584664 concerning an application u recently put in for a Bank of America Travel Rewards CC n that it was telling u to call that phone number so your application can finish being processed." RIVERA then messaged, "Before u call make sure u have the ID and social security card in front of u for ANDERSON. Also make sure u have the profiles pulled up on WhatsApp just incase they ask for your residential address, business address annual income or whatever else. Just make sure u ready for them just incase. I believe u going to hit with another card because when they send that letter out that means their considering in approving u for another CC." The following day, JOSEPH, using the "$ BLAKY $" phone number responded, "Yo i forgot to tell you, the trap needs to be paid" and "It's out of service."

17. Based on my training and experience as well as my familiarity with this investigation, I believe RIVERA obtained the A.T.L. stolen identity information and provided the identifiers and a corresponding fraudulent driver's license to JOSEPH so that he could open a bank account at Chase Bank, Bank of America and other financial institutions. I believe RIVERA applied for a credit card, online, in the A.T.L. identity on behalf of JOSEPH. RIVERA then contacted JOSEPH and directed him to use the A.T.L. burner phone to contact Bank of America to check on the status of the credit card application. JOSEPH then informed RIVERA that the burner phone did not have any minutes left on it so RIVERA would have to pay for it. Additionally, the conversation suggested JOSEPH had possession of the A.T.L. driver's license and social security card, as RIVERA reminded him to have the documents in front of him while on the phone with the bank. While agents are awaiting records from Bank of America, it appears a Bank of America account was opened in the A.T.L. identity, as RIVERA messaged JOSEPH photographs of a debit card in the A.T.L. identity. Additionally, it appears

that at some point between August 21 and September 9, the A.T.L. documents went from JOSEPH's possession to RIVERA's possession, as on September 9, 2020, RIVERA messaged the following photographs to JOSEPH at the $ BLAKY $ phone number: (a) New Jersey driver's license in the A.T.L. identity depicting JOSEPH, (b) social security card xxx-xx-1810 in the name of A.T.L., (c) Bank of America debit card ending in -4742 in the name of A.T.L., (d) reverse side of Bank of America card, (e) Chase visa card ending in 5281 in the name of A.L., and (f) reverse side of Chase card.

Confirmation of Valid Social Security Number; Identification of the Victim

18. The Social Security Administration ("SSA") has confirmed that social security number xxx-xx-1810 is assigned to A.T.L. a United States citizen from Puerto Rico.

19. The SSA has confirmed that social security number xxx-xx-1810 is not assigned to JOSEPH.

20. Law enforcement contacted the Puerto Rico Police Department to obtain the driver's license of A.T.L. with social security number xxx-xx-1810. The Puerto Rico driver's license for A.T.L. lists the name A.T.L., social security number xxx-xx-1810, and date of birth xx-xx-1976. The driver's license also displays the photograph of a man who I believe to be the real A.T.L., who is very much different in appearance than JOSEPH.

CRUZ's Acts in Furtherance of the Conspiracy and Scheme to Defraud

CRUZ's Use of R.J.T.L. Identity Generally

21. Within RIVERA's cell phone seized from 15 Brockton Ave on September 10, 2020, agents also discovered a WhatsApp conversation between RIVERA and a contact saved as "PALMA,"[10] who used cell phone number (978) 305-7514 . The conversation took place on

[10] The investigation has revealed that "Palma" is a nickname or alias that co-conspirators use for CRUZ.

September 3, 2020 when RIVERA messaged CRUZ, "Yo ur pro [profile] address reflected for RICARDO so now we can go out n play at the retail stores. Want to apply at a few stores today n see what we get."

22. On September 6, 2020, RIVERA sent the following information to CRUZ at (978) 305-7514 through WhatsApp:

> R.J.T.L.,[11] 421 Litchfield St. Apt 1, Torrington, CT 06790-6660
> Been in residence 5Y 7M
> Monthly rent: $980
> DOB: xx/xx/1980 AGE: 40
> SSN: xxx-xx-1970
> Phone: 860-278-9348
> Email: TXXXXXroofingcompany80@gmail.com
> Mailing Address: R.J.T.L., 33 Dixwell Ave, Suite #168, New Haven, CT 06511
> Business Name & Address: TXXXXX Roofing Company, 421 Litchfield St, Torrington, CT 06790
> Been in Business: 5Y 6M
> Annual Income: $203,000
> Monthly Income: $16,916
>
> Chase Bank Personal Checking Account:
> Date Opened: July 27, 2020
> Opening Deposit: $25
> Online Banking Username: Ricardoxxxx
> Password: xxxxxxxxx
> Account#: xxxxxx267
> Debit Card #: xxxx-xxxx-xxxx-3609
>
> Bank of America Personal Account:
> Date Opened: July 23, 2020
> Opening Deposit: $25
> Username: Ricardoxxxx
> Password: xxxxRicardo
> Account#: xxxx-xxxx-1898

[11] The identity of the victim, R.J.T.L., is known to the government. These initials represent the victim's first name, middle name, paternal last name and maternal last name. To protect the victim's privacy, the initials "R.J.T.L.," and "R.T.L." are used in this affidavit to reflect the variations of the victim's full name that were used by CRUZ. Likewise, the victim's last name has been redacted from the email and business name listed in the profile. The victim's first name (Ricardo) is included occasionally where necessary to convey meaning.

Debit Card #: xxxx xxxx xxxx 5376

*Palma 777

As notated in footnote 8 above, I have learned RIVERA commonly notates a version of an individual's true name/nickname below a fraudulent identity followed by what appears to be a credit score. In this case, RIVERA's notes indicated that "PALMA," a.k.a. CRUZ, was using the R.J.T.L. identity, which was associated with a 777 credit score. As described below, I believe that CRUZ used the R.J.T.L. identity to, among other things, open the above Chase Bank and Bank of America accounts and receive funds obtained through a conspiracy with RIVERA and LOPEZ.

23. On September 8, 2020, between approximately 10:21 am and 10:22 am, RIVERA sent the following messages to CRUZ at (978) 305-7514 through WhatsApp, "Yo go to the U-Haul in South by the beacons n rent a truck with the RICARDO license. A 10' or 15.' Then we link up to go get the phones." Agents contacted U-Haul and received information that customer R.T.L. of 421 Litchfield St in Torrington, CT rented a 15-foot moving van on September 8, 2020, at approximately 1:14 pm. The company provided a scanned image of Pennsylvania driver's license #42000632[12] in the name of R.J.T.L. with an issuance date of 03/27/2020 and an expiration date of 04/11/2024 related to the rental. The license photograph clearly depicts CRUZ.

CRUZ's Use of R.J.T.L. Identity to Open Fraudulent Bank Account

24. On or about July 27, 2020, at approximately 12:39 pm, a man appeared in person at a Chase bank branch in Hartford, Connecticut and provided personal identifying

[12] Due to a reflection on the driver's license, some digits of the license number are difficult to read. However, 42000632 is the number I believe to be on the document.

information on a bank application in order to open a Chase total checking account. On the application, the applicant represented himself as R.J.T.L with a date of birth of xx-xx-1980 and social security number xxx-xx-1970. The applicant provided an address of 421 Litchfield St., Apt 1 Torrington, CT, and phone number 860-278-9348 (the R.J.T.L. burner phone number sent from RIVERA). During the account opening process, the applicant presented a Pennsylvania driver's license with license number 4000632, date of birth of xx-xx-1980, issuance date of 03/27/2020, and expiration date of 04/11/2024. The applicant also provided a social security card bearing social security number xxx-xx-1970. After obtaining from U-Haul the Pennsylvania driver's license in the R.J.T.L. identity but depicting CRUZ's face and comparing them to the documentation provided by the applicant at Chase Bank, agents determined the license number[13], issue date, expiration date and social security number are the same. The applicant successfully opened checking account #xxxxxx267 with Chase Bank. Additionally, agents received video surveillance footage from Chase bank based on a request for video/images related to account #xxxxxx267. The video surveillance depicts CRUZ, who is identified by his body type, partial face shots and tattoos, conduct a transaction with a Chase employee; the timestamp of the video where CRUZ is visible is July 27, 2020 between 12:49 and 12:52 pm.

25. Based on my training and experience as well as my familiarity with this investigation, I believe RIVERA obtained the R.J.T.L. stolen identity information and provided the identifiers and a corresponding fraudulent driver's license to CRUZ so that he could open a bank account at Chase Bank and other financial institutions. Additionally, it appears that

[13] The license number contains one less digit from the scanned license image agents received from U-Haul, however all remaining digits are the same.

CRUZ may still be in possession of these documents, as a vehicle was rented using the identity of R.T.L., of 421 Litchfield St. Torrington, Connecticut, on September 10, 2020, several hours after eight individuals connected to this investigation were arrested. The individual purporting to be R.T.L. presented Pennsylvania driver's license # 42000632 (the license presented to Chase Bank and to U-Haul) and paid with Chase Visa card xxxx-xxxx-xxxx-3609 (the Chase account discussed above) and provided phone number 860-278-9348 (the $ RICARDO $ burner phone).

26. Notably, CRUZ opened the R.J.T.L. Chase Bank account at the Hartford, CT branch on July 27, 2020 at approximately 12:39 pm, and JOSEPH opened the A.T.L. Chase Bank account at the Avon, CT branch the same day at approximately 2:00 pm. According to Google Maps, these locations are approximately fifteen to twenty minutes from one another. Based on this information as well as my knowledge of this investigation, I believe both JOSEPH and CRUZ coordinated the opening of their respective Chase Bank accounts and did so under the direction of RIVERA.

CRUZ's Use of R.J.T.L. Identity in Connection with Fraudulent Bank Transactions in Furtherance of Conspiracy

27. On August 18, 2020, an individual using a "K.N."[14] Chime/Stride Bank account made two payments/transfers, in the amount of $4,000 and $500 respectively, to the R.J.T.L. Chase account. Most of this money was withdrawn from the R.J.T.L. Chase account the same day or the next day; on August 18, 2020, $503 was withdrawn, and on August 19, 2020 $3,900 was withdrawn from the Chase account.

28. During the search of RIVERA's residence at 15 Brockton Ave, agents located

[14] The identity of the victim, K.N., is known to the government. These initials represent the victim's first name and last name.

and seized Chime Debit Card xxxx-xxxx-xxxx-5252 in the name of K.N. Agents subsequently learned that an EIDL from the SBA totaling $44,000 had been deposited into the account associated with the card on or about August 4, 2020. Chime Financial produced records for this account showing that the card had a balance of 87 cents as of August 31, 2020; most of the funds had been expended on Apple iPhones in New Hampshire, while some transactions originated in Haverhill, MA.

29. Also at RIVERA's residence, agents located a fraudulent Georgia driver's license in the name of K.N., which depicted LOPEZ.

30. Further review of RIVERA's cellphone revealed a WhatsApp conversation between RIVERA and "MOM" (believed to be LOPEZ, based on the context set forth below), which took place between approximately 4:19 pm and 4:33 pm on August 18, 2020, the same day the person-to-person payment was made from K.N.'s Chime/Stride Bank account to the R.J.T.L. Chase account. Below is a summary of the conversation:

MOM	Yo it's the same guy
RIVERA	Fuck
MOM	And they took the ID
MOM	To a banker in the back
MOM	I'm gonna see what I do. If I pull this off u sooo owe me
RIVERA	U should've told them why they taking your ID
MOM	Palma spoke not me
RIVERA	WTF u know we never allow that
RIVERA	Try to show the girl your chime card n the chime account on your phone showing u linked the card to your chime to transfer the money

RIVERA	That u only there to clarify the money transfer from your chime account to Mr. Ricardo's Chase account n that's all

31. Based on my training and experience, as well as my knowledge of this investigation, I believe that this conversation occurred while LOPEZ (using K.N.'s identity) was at a bank with CRUZ (using R.J.T.L.'s identity). LOPEZ was first informing RIVERA that an employee was working with whom she had used another stolen identity and she was concerned he would recognize her. She then informed RIVERA that bank employees took the identity document she and "Palma" (CRUZ) had presented. RIVERA then becomes upset, saying "they" should never allow bank employees to physically take an identity document and she should have asked why they needed her identity document. LOPEZ informed RIVERA that "Palma" (CRUZ), was doing all the talking. RIVERA suggested that LOPEZ tell bank employees that she was trying to transfer money from her Chime account to "Mr. Ricardo's Chase Account."

32. Bank records show the transfer was successful, as two person-to-person payments were conducted on August 18, 2020 from the K.N. Chime/Stride Bank account to the R.J.T.L. Chase account. I believe that LOPEZ and CRUZ were representing themselves to be K.N. and R.J.T.L. and were attempting to transfer funds from one fraudulent account to another under the direction of RIVERA and in furtherance of their conspiracy.

33. Additionally, in RIVERA's iPhone that was seized on September 10, 2020, agents located another messaging conversation that RIVERA engaged in on August 18, 2020, this time with the "$ RICARDO $" burner phone at 860-278-9348, which is the same phone number associated with the R.J.T.L. profile that RIVERA messaged CRUZ. At approximately 1:56 pm, $ RICARDO $ messaged RIVERA, "I'm next up in the teller," to which RIVERA responded, "the balance is there, $4,520." RIVERA then sent a series of messages providing an

explanation for $ RICARDO $ to provide to the bank teller about why he was withdrawing the money and where the money came from. RIVERA told $ RICARDO $ to explain the money was "a first and last security payment for an apartment you are renting to K.N." He told $ RICARDO $ that if they called K.N., RIVERA had the phone and would answer like he was her husband. RIVERA and $ RICARDO $ then conversed for approximately 20 minutes about $ RICARDO $ having issues withdrawing the money. The conversation then picked up approximately two hours later, when $ RICARDO $ appeared to be attempting to withdraw money yet again, when he messaged to RIVERA, "If they try to scan them ID's its gonna be problematic." At approximately 5:29 pm, $ RICARDO $ messaged, "They trynna verify signatures" to which RIVERA messaged back, "WTF" and "Sign how u always sign bro."

Confirmation of Valid Social Security Number; Identification of the Victim

34. The SSA has confirmed that social security number xxx-xx-1970 is assigned to R.J.T.L. a United States citizen from Puerto Rico.

35. The SSA has confirmed that social security number xxx-xx-1970 is not assigned to Ramon Joseph CRUZ.

36. Law enforcement contacted the Puerto Rico Police Department to obtain the driver's license of R.J.T.L. with social security number xxx-xx-1970. The Puerto Rico driver's license for R.J.T.L. lists the name R.J.T.L., social security number xxx-xx-1970, and date of birth xx-xx-1980. The driver's license also displayed the photograph of a man who I believe to be the real R.J.T.L. who is very much different in appearance than CRUZ.

Defendants' Involvement with Fraudulent Economic Injury Disaster Loans In Furtherance of Conspiracy

37. Based on the investigation to date, described further below, as well as my training and experience, I believe probable cause exists to believe that JOSEPH and CRUZ

assisted RIVERA in a conspiracy to steal the identities of actual United States citizens, use their personal information to apply for EIDLs from the SBA, to receive at their Massachusetts residences Chime cards linked to bank accounts containing the fraudulently-obtained EIDL funds, and to launder the stolen funds, using interstate wires in furtherance of the conspiracy. I form this opinion based on my training and experience and based upon a number of factors, including JOSEPH's and CRUZ's involvement in opening fraudulent bank accounts which were linked to stolen EIDLs, their receiving in the mail Chime cards connected to bank accounts containing stolen EIDL funds, their laundering of funds from the Chime accounts by purchasing iPhones for re-sale, and many of their communications with RIVERA.

38. As discussed in detail above, JOSEPH opened an account with Chase Bank on or about July 27, 2020. Bank records show no activity occurred within the checking account thereafter, aside from a $25 deposit for the account opening and various fees. As of November 4, 2020, the account contained a negative $4.00 balance. Additionally, as discussed in detail above, CRUZ also opened an account with Chase Bank on or about July 27, 2020. Bank records show minimal activity within that checking account aside from the two person-to-person payments conducted on August 18, 2020 from the K.N. Chime card to the R.J.T.L. Chase account as discussed in paragraphs 27 through 32 above. Based on my familiarity with the scheme, it is my opinion that both JOSEPH and CRUZ opened checking accounts with Chase bank (1) to apply for credit cards with Chase bank and purchase merchandise on credit that would never be paid back; and (2) so that RIVERA and others could link the accounts to other fraudulent accounts for the purpose of accepting money transfers, such as from Chime/Stride

Bank accounts in the name of C.M.,[15] T.B.,[16] D.C., and K.N.

39. During the search of RIVERA's residence at 15 Brockton Ave, agents located and seized Chime Debit Card xxxx-xxxx-xxxx-7515 in the name of C.M. Agents subsequently learned that $45,300 in funds from an SBA EIDL had been deposited into the account associated with that card on or about August 4, 2020. Chime Financial records for this account show that the account contained a linked Automatic Clearing House ("ACH") account, which was Chase Bank account number xxxxxx360 – the account that, as described in paragraphs 13 and 14, JOSEPH had opened in the A.T.L. identity. On September 23, 2020, Chime Financial disabled the account due to "synthetic ID account suspected."

40. During the search of RIVERA's residence at 15 Brockton Ave, agents also located and seized Chime Debit Card xxxx-xxxx-xxxx-1381 in the name of T.B. Agents subsequently learned that $44,800 in funds from an SBA EIDL had been deposited into the account associated with the card on or about August 3, 2020. Agents discovered the account contained a linked ACH account, which was Bank of America account number xxxx-xxxx-1335, the A.T.L. account described above in paragraphs 15 through 17. On September 15, 2020, Chime Financial disabled the account due to "synthetic ID account suspected."

41. As discussed in paragraph 27, agents located and seized Chime Debit Card xxxx-xxxx-xxxx-5252 in the name of K.N. during the search warrant conducted 15 Brockton Ave. Agents learned the account contained a linked ACH account, which was Chase Bank account number xxxxxx267 – the R.J.T.L. account opened by CRUZ, as described above in paragraphs 24 through 26. On September 2, 2020, Chime Financial suspended the account due to "Load

[15] The identity of victim C.M. is known to the government. In order, these initials represent the victim's first name and last name.
[16] The identity of victim T.B. is known to the government. In order, these initials represent the victim's first name and last name.

fraud suspected."

42. As mentioned in paragraph 9, a New Hampshire driver's license in the name of D.P.C. which depicted JOSEPH, was located and seized from 15 Brockton Ave. The notes section in RIVERA's cell phone suggest there was also a Chime account in the name of D.P.C. Chime Financial records indicate that $29,100 in funds from an SBA EIDL had been deposited into the account associated with the D.P.C. Chime card on or about August 4, 2020. Agents learned the account contained a linked ACH account, which was Bank of America account number xxxx-xxxx-1898 – the R.J.T.L. account whose details RIVERA sent in a message to CRUZ, as described above in paragraph 22.

43. In total, agents identified approximately $452,204 in SBA funds that had been sent to Chime accounts associated with Chime debit cards that were seized from 15 Brockton Ave and/or whose account details were stored in RIVERA's phone. Chime records indicated approximately $250,000 of this money was used to purchase iPhones at Apple stores in Massachusetts and New Hampshire, which I believe were then re-sold for cash.

44. Agents contacted Apple for transaction details related to the Chime accounts referenced throughout this affidavit. In December 2020, agents received detailed records of hundreds of transactions that took place between August 14, 2020 and September 9, 2020. The product description of every transaction was an iPhone 11 Pro Max 256 gigabyte phone with an original price of $1,249. Apple results also revealed several different Chime cards were used to make the purchases, often within minutes of one another, and from the same store.

45. For example, on September 9, 2020 – the day before the arrests of RIVERA and several of his co-conspirators –12 apple iPhone 11s were purchased from the Rockingham Park Apple store in New Hampshire. Video surveillance showed an individual who appears similar in

appearance to JOSEPH, and an individual confirmed to be CRUZ,[17] walk into the Apple store within one minute of each other and wait in line. JOSEPH and CRUZ stood a few feet apart and did not appear to communicate or make eye contact. Video surveillance showed CRUZ, who was wearing a dark blue hat, purchase two iPhones, and then purchase another two iPhones in a separate transaction. While CRUZ was making the purchases, the individual believed to be JOSEPH, who was wearing a light blue hat, made a purchase of two iPhones at the same table but with a different sales associate. He then made a second transaction purchasing two more iPhones and then departed the store. CRUZ remained at the table and purchased an additional two iPhones and then departed the store.

46. When agents compared and cross-referenced the time of the transactions with the video footage from Apple, it was apparent the individuals believed to be JOSEPH and CRUZ used the fraudulently-obtained Chime cards to purchase ten iPhones. Specifically, JOSEPH used Chime card xxxx-xxxx-xxxx-2359 in the name of H.F.[18] for his first transaction, and he used Chime card xxxx-xxxx-xxxx-6306 in the name of B.M.[19] for the second transaction. CRUZ used Chime card xxxx-xxxx-xxxx-3769 in the name of C.C.[20] for his first transaction, and he used Chime card xxxx-xxxx-xxxx-0916 in the name of R.O.[21] for the second transaction. All but one of these Chime cards were seized during the execution of the search warrant at 15 Brockton Avenue the very next day. Additionally, records for the accounts associated with the

[17] Although the first individual appears the same in stature and appearance as JOSEPH, he was wearing a mask and a hat, making it more difficult to definitively physically identify him. However, based on all of the information set forth in this affidavit, I believe he is JOSEPH. CRUZ was readily identified by his tattoos, which were visible.
[18] The identity of victim H.F. is known to the government. In order, these initials represent the victim's first name and last name.
[19] The identity of victim B.M. is known to the government. In order, these initials represent the victim's first name and last name.
[20] The identity of victim C.C. is known to the government. In order, these initials represent the victim's first name and last name.
[21] The identity of victim R.O. is known to the government. In order, these initials represent the victim's first name and last name.

R.O., H.F., and C.C. Chime cards all indicate that the cards were used at Apple stores in Massachusetts, sometimes within minutes of each other.

47. I understand, based on this investigation, as well as my training and experience, that debit card transactions generally involve (1) the presentation of a debit card at a point of sale, (2) the "swiping" or reading of the debit card at the point of sale, and (3) the transmission of data about the transaction, via an internet connection or telephone line (i.e., through interstate wires), to the relevant bank or processor in order to confirm that the bank account with which the debit card is associated has sufficient funds for the transaction, and to commence the exchange of funds and effectuate the sale. Chime Financial/ Stride Bank utilizes a payment processor by the name of Galileo Technologies, which utilizes servers in Illinois, California, New Jersey, and Utah to process debit card transactions. The bulk of the Chime card purchases made in furtherance of this conspiracy took place in Massachusetts and New Hampshire. Accordingly, the Chime debit card transactions originating in Massachusetts and New Hampshire all involved interstate wires.

Repeated Use of Fraudulent Identities

48. Throughout the course of this investigation, agents have uncovered identity documents in various identities that depict JOSEPH. In addition to the three driver's licenses mentioned in this affidavit, in April 2020, agents became aware of a Pennsylvania driver's license that was seized at a Days Inn hotel in connection with this investigation. The driver's license depicted JOSEPH, yet was in the name of an individual who had the initials A.E.T.M.

49. Agents also have a still image of JOSEPH attempting to open a bank account

with a Southern Maine Bank[22] on or about February 19, 2020. It appears JOSEPH opened an account in the name of R.L.R.F.[23] and made a deposit of $25. The bank maintained scanned copies of a Pennsylvania driver's license and a social security card, each in the name of R.L.R.F., and the driver's license photo depicted JOSEPH. Agents identified a second instance of fraud when JOSEPH applied for a Key cashback credit card on February 18, 2020, and March 7, 2020, in Kittery, ME. In connection with those transactions, JOSEPH presented what appeared to be the same Pennsylvania driver's license and social security card in the R.L.R.F. identity. In the photograph on the Pennsylvania driver's license, JOSEPH appears to be wearing a light-colored collared shirt. Agents discovered what appears to be the same mugshot-style photograph as appeared on the Pennsylvania driver's license, stored in RIVERA's laptop that was seized from 15 Brockton Ave. on September 10.

50. Agents also discovered a mugshot-style photograph of JOSEPH in RIVERA's cell phone that was seized from Brockton Ave. In the photograph, JOSEPH is wearing a white crewneck t-shirt with a wrinkled collar. This mugshot appears to be the same image as appears on the A.T.L. New Jersey license mentioned throughout this affidavit. Additionally, in a cellphone seized from RIVERA in January 2019 (*see* Exhibit 1, ¶¶ 14-15 for details regarding the search and seizure of that phone), agents located a third mugshot-style photograph of JOSEPH in which he is wearing a white V-neck t-shirt.

51. Similarly, agents discovered a mugshot-style photograph of CRUZ in RIVERA's cell phone that was seized from 15 Brockton Ave. In the photograph, CRUZ is wearing a white/light blue tie-dye t-shirt and a gold chain can be seen on his neck. Also discovered within

[22] This is the same bank and branch that co-conspirator Neida LOPEZ opened an account with approximately nine days later.
[23] The identity of victim R.L.R.F. is known to the government. In order, these initials represent the victim's first name, middle name and paternal last name and maternal last name.

the phone was a New Hampshire driver's license in the name of D.K.K.[24] The photograph on the identification document is that of CRUZ, who is wearing a white crewneck t-shirt. The address listed on the license is an address at which agents executed a search warrant on September 10, 2020, in connection with this investigation. Additionally, there is a note in RIVERA's cell phone that suggests that a Chime account in the name of D.K.K. was in the process of being opened; RIVERA had listed PII and financial information related to D.K.K. in his phone, as he had done for several other stolen identities associated with Chime accounts.

52. Based on the above information as well as my familiarity with this investigation, I believe JOSEPH and CRUZ have been conspiring with RIVERA, LOPEZ, and others to commit various types of fraud for quite some time.

Probable Cause That Evidence, Fruits, and Instrumentalities of the Target Offenses Will Be Found at Target Location 1

53. JOSEPH has a Massachusetts driver's license on file with the Massachusetts Registry of Motor Vehicles. On file is driver's license number Sxxxx0216 in the name of Darwyn JOSEPH with a listed primary contact address of 445 S Broadway Lawrence, MA 01843.

54. Chime records show the address on file for the H.F. account (used by JOSEPH to purchase iPhones on September 9) was 445 S Broadway Lawrence, MA 01843 (Target Location 1 – JOSEPH's residence). Additionally, one of the notes in RIVERA's cell phone implied the H.F. Chime card was to be mailed to "BLAKY" (a.k.a. JOSEPH) at "445 S Broadway Lawrence, MA 01843" and expected to arrive on September 1, 2020.[25]

[24] The identity of victim D.K.K. is known to the government. In order, these initials represent the victim's first name, middle name and last name.

[25] It appears September 1, 2020 was the date RIVERA expected the H.F. Chime card to arrive at 445 S Broadway (although, in fact, it appears to have arrived no later than August 27, 2020). A note within RIVERA's phone listed the names on several Chime cards. Each card had a corresponding address, name or nickname and date. Based on

55. On November 5, 2020, at approximately 10:00 am, while conducting physical surveillance of 445 S Broadway Lawrence, MA, DBFTF agents observed JOSEPH and CRUZ exit the side door of the residence and enter a gray Cadillac sport utility vehicle (SUV), with New York registration JKE3715, that had been rented by CRUZ in September (the "Cadillac").[26] Both individuals then departed the area in the vehicle.

56. On November 6, 2020, at approximately 2:10 pm, while conducting physical surveillance of 445 S Broadway Lawrence, MA, DBFTF agents observed CRUZ arrive in the Cadillac and remain in the vehicle. Agents then observed JOSEPH exit the side door of 445 S Broadway, enter the Cadillac and depart the area.

57. The Postal Inspection Service confirmed JOSEPH received United States Postal Service (USPS) mail at 445 S Broadway as recently as December 16, 2020.

58. As mentioned above, a Chime card containing fraudulent funds in the name of H.F. was associated with, and mailed to 445 S Broadway Lawrence, MA, and subsequently used by someone who appeared to be JOSEPH.

Probable Cause That Evidence, Fruits, and Instrumentalities of the Target Offenses Will Be Found at Target Location 2

59. Chime records disclosed the address on file for the C.C. account used by the

---

my familiarity with this investigation as well as certain WhatsApp conversations in RIVERA's phone, I know the addresses listed were the addresses RIVERA expected the Chime cards to arrive at, the name or nickname was who was to receive the card on his behalf and the date was the expected arrival date of the cards.

[26] On November 5, 2020, agents received information from Hertz that the Cadillac had been rented by R.T.L. of 421 Litchfield, Torrington, Connecticut on September 10, 2020, the date that 8 individuals connected to this investigation were arrested. The individual purporting to be R.T.L. paid with Chase Visa card xxxx-xxxx-xxxx-3609 (the account discussed in paragraph 22) and provided 860-278-9348 (the number associated with the R.J.T.L. "profile" discussed in paragraph 22, and with $ RICARDO $ as discussed in paragraph 33) as his phone number. He was supposed to return the vehicle on October 6, 2020. Hertz informed agents that the vehicle was not returned, payment was overdue and an attempt at payment was conducted on November 5, 2020, which was returned as denied. Hertz also suspected that the global positioning system device on the Subject Vehicle had been tampered with. As of December 17, 2020, the Subject Vehicle still had not been returned to Hertz. As described further below, on December 2, 2020, around 1pm, the Cadillac was stopped by Methuen police for excessive speed; CRUZ was the driver, and provided a Massachusetts driver's license in his true identity. HSI obtained a tracker warrant for the Cadillac on December 10. *See* 20-MJ-6762-MPK.

individual believed to be CRUZ to purchase iPhones on September 9 was 104 Perry Ave., Apt 1 Methuen, MA (the address that appears on CRUZ's driver's license). A note in RIVERA's phone implied the C.C. Chime card was to be mailed to "Palma" (a.k.a. CRUZ) at "104 Perry Ave., Apt 1 Methuen, MA 01844" on September 1, 2020; and, indeed, the C.C. Chime card was first used on September 1, 2020. Based on the investigation, and as described further below, I believe that CRUZ recently moved from 104 Perry Avenue in Methuen to 66 Pleasant Street 2 in Methuen.

60. On November 12, 2020, at approximately 2:00 pm, while conducting physical surveillance of 66 Pleasant St., Methuen, MA, DBFTF agents observed CRUZ exit the second floor side door of the residence and enter the Cadillac. CRUZ then departed the area in the vehicle.

61. On November 19, 2020, at approximately 11:00 am, while conducting physical surveillance of 66 Pleasant St., DBFTF agents observed CRUZ exit the second floor side door of the residence, enter the Cadillac, and depart the area.

62. On December 2, 2020, at approximately 1:00 pm, DBFTF agents observed CRUZ exit the second floor side door of 66 Pleasant St and depart in the Cadillac as the sole occupant. Within minutes, CRUZ was stopped by Methuen police for driving over the speed limit. CRUZ provided police with a MA driver's license bearing license number Sxxxx1303 and a United States Army photo ID in the name of CRUZ. During the stop, CRUZ informed officers that he had recently moved into 66 or 68 Pleasant Street[27] and that he was driving a rental. 66 Pleasant Street is a completely different structure than 68 Pleasant Street, and DBFTF

[27] It was unclear as to whether the Methuen police officer who spoke with CRUZ could not remember if CRUZ said he lived at 66 or 68 Pleasant Street or if CRUZ stated he lived at "66 or 68 Pleasant Street."

agents have seen CRUZ exit 66 Pleasant Street on numerous occasions.

63. On December 18, 2020, the Postal Inspection Service confirmed that CRUZ receives mail at 66 Pleasant Street 2.

64. An internet real estate listing from 2014 indicates that 66 Pleasant Street was at that time being used as a single family home, but could also be used as a two-family home. Photos of the interior of the residence from that time show an internal staircase from inside the first floor living area, believed to lead up to the second-floor living area. I believe that the first floor living area is currently being used by a family member of CRUZ's, and that CRUZ is primarily using the second floor living area. However, given the layout of the home, I believe that there are common areas within 66 Pleasant Street to which CRUZ also has access.

65. I know, based on my training and experience, that:

a. Individuals often keep identification documents and financial records and other evidence of identity for long periods – sometimes years – and tend to retain such documents even when they depart a given residence. Such documents include driver's licenses, social security cards, bank cards, credit cards, bank records, and credit card statements.

b. Individuals often keep identification documents and financial records in their residence, in part to ensure the security of these documents and in part to allow for access to these documents when needed.

c. In addition, it is common for those who use other persons' identities without authorization to maintain fraudulently obtained identification documents in secure locations within their residence to conceal them from law enforcement authorities;

d. It is common for individuals who use fraudulently obtained identification documents to retain those documents for substantial periods of time so that they can continue to use the fraudulently obtained identities;

e. Individuals involved in making false identification documents often use computers, cell phones, printers, and similar equipment to create the false identification documents. This equipment is often stored in the individual's home. This equipment is expensive and durable, and can be stored and used for years; and

f. Based on my experience and training, I also know that individuals who make purchases of goods and services often retain their receipts and invoices in their residence.

66. I also know, based on my training and experience:

a. Individuals frequently use computer equipment to carry out, communicate about, and store records regarding their daily activities. These tasks are frequently accomplished through sending and receiving e-mail, instant messages, and other forms of phone or internet based messages; scheduling activities; keeping a calendar of activities; arranging travel; purchasing items; searching for information including information regarding travel and activities; arranging for travel, accessing personal accounts including banking information; paying for items; and creating, storing, and transferring images, videos, and other records of their movements and activities.

b. Individuals involved in criminal activity, to include the planning and

execution of identity theft schemes, communicate with each other through the use of cellular telephones. Additionally, I am also aware that individuals involved in criminal activity, to include the planning and execution of identity theft schemes, communicate using social media networking sites like Facebook, Snapchat, WhatsApp, etc. which can be accessed through cellular telephones.

c. I know that many smartphones (which are included in Attachment B-1 and B-2's definition of "hardware") can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

d. I am aware that individuals commonly store records of the type described in Attachment B-1 and B-2 in mobile phones, computer hardware, computer software, and storage media.

e. I know that data can often be recovered months or even years after it has been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

i. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their electronic equipment, they can easily transfer

the data from their old device to a new one.

ii. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file often does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, the device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

iii. Wholly apart from user-generated files, electronic storage media often contains electronic evidence of how the device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but users typically do not erase or delete this evidence because special software is typically required for that task.

iv. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed

Internet pages or if a user takes steps to delete them.

v. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

vi. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g.,

registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both

show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

vii. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

viii. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that

are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

ix. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

67. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

68. The premises may contain computer equipment whose use in the crimes or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B-1 and B-2 are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

69. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied, or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Conclusion

70. Based on the foregoing, I submit there is probable cause to believe that, Darwyn JOSEPH and Ramon Joseph CRUZ (1) on or about July 27, 2020, knowingly transferred, possessed and used, during and in relation to any felony violation enumerated in 18 U.S.C. 1028A(c), and without lawful authority, a means of identification of another person in violation

of 18 U.S.C. § 1028A; and (2) between July 27, 2020 and December 17, 2020, having conspired with others known and unknown to commit wire fraud, that is, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, which schemes involved the transmission by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing the scheme to defraud, to include, stolen identity information to Chase Bank, Chime Financial, Stride Bank, and Galileo Technologies, in violation of Title 18, United States Code, § 1343, all in violation of 18 U.S.C. § 1349.

71. Based on the forgoing, I have probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachments B-1 and B-2, are located in the premises described in Attachments A-1 and A-2.

Signed under the pains and penalties of perjury this 18th day of December, 2020.

/s/ Jacqleen Cunningham

Jacqleen M. Cunningham
Special Agent
Homeland Security Investigations

Subscribed and sworn to via telephone in accordance with Federal Rule of Criminal Procedure 4.1 this 18th day of December, 2020.

HONORABLE M. PAGE KELLEY
CHIEF UNITED STATES MAGISTRATE JUDGE
DISTRICT OF MASSACHUSETTS